IPE JC110
NOV 3 0 2000
PATENT & TRADEMARK OFFICE

RECEIVED
DEC 0 6 2000
Technology Center 2600

D. Gail. #7 12-8-00 2681

S/N 09/627684

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Rajaniemi		
Serial No.:	09/627684	Group Art Unit:	2744
Filed:	7/28/00	Docket No.:	975.311USW1
Title:	A METHOD FOR A SECURE DETACH PROCEDURE IN A RADIO TELECOMMUNICATION NETWORK		

CERTIFICATE UNDER 37 C.F.R. 1.8: The undersigned hereby certifies that this Transmittal Letter and the paper, as described herein, are being deposited in the United States Postal Service as first class mail, with sufficient postage, in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231 on November 27, 2000.

Michael B. Lasky
Name

Signature

Group Art Unit 2744
Assistant Commissioner for Patents
Washington, D.C. 20231

☒ Certified copy of WIPO Serial Number PCT/EP 98/08064, filed 10 December 1998; Submission of Priority Document
☒ Transmittal Sheet
☒ Return postcard

Authorization is hereby given to charge any additional fees or credit any overpayments that may be deemed necessary to Deposit Account Number 50-1038.

Respectfully submitted,

Altera Law Group, LLC
10749 Bren Road East, Opus 2
Minneapolis, MN 55343

By: _____
Michael B. Lasky
Reg. No. 29,555

Date: Nov. 27, 2000

PE
NOV 3 0 2000
PATENT & TRADEMARK OFFICE

RECEIVED
DEC 0 6 2000
Technology Center 2600

S/N 09/627684

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Rajaniemi		
Serial No.:	09/627684	Group Art Unit:	2744
Filed:	7/28/00	Docket No.:	975.311USW1
Title:	A METHOD FOR A SECURE DETACH PROCEDURE IN A RADIO TELECOMMUNICATION NETWORK		

CERTIFICATE UNDER 37 C.F.R. 1.8: The undersigned hereby certifies that this Transmittal Letter and the paper, as described herein, are being deposited in the United States Postal Service, as first class mail, with sufficient postage, in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231 on November 27, 2000.

Michael B. Lasky
Name

Signature

SUBMISSION OF PRIORITY DOCUMENT

Group Art Unit 2744
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Enclosed is a certified copy of WIPO application, Serial Number PCT/EP 98/08064, filed 10 December 1998, the priority of which is claimed under 35 U.S.C. §120.

Respectfully submitted,

Altera Law Group, LLC
10749 Bren Road East, Opus 2
Minneapolis, MN 55343

By:
Michael B. Lasky
Reg. No. 29,555

Date: November 27, 2000

Europäisches Patentamt | European Patent Office | Office européen des brevets

OIPE JC110
NOV 30 2000
PATENT & TRADEMARK OFFICE

Bescheinigung

Certificate

Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten internationalen Patentanmeldung überein.

The attached documents are exact copies of the international patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet international spécifiée à la page suivante.

RECEIVED
DEC 06 2000
Technology Center 2600

Den Haag, den
The Hague,
La Haye, le 27. 10. 2000

Der Präsident des Europäischen Patentamts
Im Auftrag
For the President of the European Patent Office
Le Président de l'Office européen des brevets
p.o.

C. van Amstel

Patentanmeldung Nr.
Patent application no.
Demande de brevet n° PCT/EP 98/08064

Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation

Anmeldung Nr.:
Application no.:
Demande n°: PCT/EP 98/08064

Anmelder:
Applicant(s):
Demandeur(s): 1. NOKIA NETWORKS OY - Nokia Group, Finland
2. RAJANIEMI, Jaakko - Helsinki, Finland

Bezeichnung der Erfindung:
Title of the invention:
Titre de l'invention: A method for secure detach procedure in a radio telecommunication network

Anmeldetag:
Date of filing:
Date de dépôt: 10 December 1998 (10.12.98)

In Anspruch genommene Priorität(en)
Priority(ies) claimed
Priorité(s) revendiquée(s)

Staat:	Tag:	Aktenzeichen:
State:	Date:	File no.
Pays:	Date:	Numéro de dépôt:

Benennung von Vertragsstaaten : Siehe Formblatt PCT/RO/101 (beigefügt)
Designation of contracting states : See Form PCT/RO/101 (enclosed)
Désignation d'états contractants : Voir Formulaire PCT/RO/101 (ci-joint)

Bemerkungen:
Remarks:
Remarques:

Feld Nr. V BESTIMMUNG VON STAATEN

Die folgenden Bestimmungen nach Regel 4.9 Absatz a werden hiermit vorgenommen *(bitte die entsprechenden Kästchen ankreuzen: wenigstens ein Kästchen muß angekreuzt werden)*:

Regionales Patent

- ☒ AP **ARIPO-Patent:** **GH** Ghana, **GM** Gambia, **KE** Kenia, **LS** Lesotho, **MW** Malawi, **SD** Sudan, **SZ** Swasiland, **UG** Uganda, **ZW** Simbabwe und jeder weitere Staat, der Vertragsstaat des Harare-Protokolls und des PCT ist
- ☒ EA **Eurasisches Patent:** **AM** Armenien, **AZ** Aserbaidschan, **BY** Belarus, **KG** Kirgisistan, **KZ** Kasachstan, **MD** Republik Moldau, **RU** Russische Föderation, **TJ** Tadschikistan, **TM** Turkmenistan und jeder weitere Staat, der Vertragsstaat des Eurasischen Patentübereinkommens und des PCT ist
- ☒ EP **Europäisches Patent:** **AT** Österreich, **BE** Belgien, **CH und LI** Schweiz und Liechtenstein, **CY** Zypern, **DE** Deutschland, **DK** Dänemark, **ES** Spanien, **FI** Finnland, **FR** Frankreich, **GB** Vereinigtes Königreich, **GR** Griechenland, **IE** Irland, **IT** Italien, **LU** Luxemburg, **MC** Monaco, **NL** Niederlande, **PT** Portugal, **SE** Schweden und jeder weitere Staat, der Vertragsstaat des Europäischen Patentübereinkommens und des PCT ist
- ☒ OA **OAPI-Patent:** **BF** Burkina Faso, **BJ** Benin, **CF** Zentralafrikanische Republik, **CG** Kongo, **CI** Côte d'Ivoire, **CM** Kamerun, **GA** Gabun, **GN** Guinea, **ML** Mali, **MR** Mauretanien, **NE** Niger, **SN** Senegal, **TD** Tschad, **TG** Togo und jeder weitere Staat, der Vertragsstaat der OAPI und des PCT ist *(falls eine andere Schutzrechtsart oder ein sonstiges Verfahren gewünscht wird, bitte auf der gepunkteten Linie angeben)* GW Guinea-Bissau

Nationales Patent *(falls eine andere Schutzrechtsart oder ein sonstiges Verfahren gewünscht wird, bitte auf der gepunkteten Linie angeben)*:

- ☒ AL Albanien
- ☒ AM Armenien
- ☒ AT Österreich
- ☒ AU Australien
- ☒ AZ Aserbaidschan
- ☒ BA Bosnien-Herzegowina
- ☒ BB Barbados
- ☒ BG Bulgarien
- ☒ BR Brasilien
- ☒ BY Belarus
- ☒ CA Kanada
- ☒ CH und LI Schweiz und Liechtenstein
- ☒ CN China
- ☒ CU Kuba
- ☒ CZ Tschechische Republik
- ☒ DE Deutschland
- ☒ DK Dänemark
- ☒ EE Estland
- ☒ ES Spanien
- ☒ FI Finnland
- ☒ GB Vereinigtes Königreich
- ☒ GE Georgien
- ☒ GH Ghana
- ☒ GM Gambia
- ☐ ~~GW Guinea-Bissau~~
- ☒ HR Kroatien
- ☒ HU Ungarn
- ☒ ID Indonesien
- ☒ IL Israel
- ☒ IS Island
- ☒ JP Japan
- ☒ KE Kenia
- ☒ KG Kirgisistan
- ☒ KP Demokratische Volksrepublik Korea
- ☒ KR Republik Korea
- ☒ KZ Kasachstan
- ☒ LC Saint Lucia
- ☒ LK Sri Lanka
- ☒ LR Liberia
- ☒ LS Lesotho
- ☒ LT Litauen
- ☒ LU Luxemburg
- ☒ LV Lettland
- ☒ MD Republik Moldau
- ☒ MG Madagaskar
- ☒ MK Die ehemalige jugoslawische Republik Mazedonien
- ☒ MN Mongolei
- ☒ MW Malawi
- ☒ MX Mexiko
- ☒ NO Norwegen
- ☒ NZ Neuseeland
- ☒ PL Polen
- ☒ PT Portugal
- ☒ RO Rumänien
- ☒ RU Russische Föderation
- ☒ SD Sudan
- ☒ SE Schweden
- ☒ SG Singapur
- ☒ SI Slowenien
- ☒ SK Slowakei
- ☒ SL Sierra Leone
- ☒ TJ Tadschikistan
- ☒ TM Turkmenistan
- ☒ TR Türkei
- ☒ TT Trinidad und Tobago
- ☒ UA Ukraine
- ☒ UG Uganda
- ☒ US Vereinigte Staaten von Amerika
- ☒ UZ Usbekistan
- ☒ VN Vietnam
- ☒ YU Jugoslawien
- ☒ ZW Simbabwe

Kästchen für die Bestimmung von Staaten (für die Zwecke eines nationalen Patents), die dem PCT nach der Veröffentlichung dieses Formblatts beigetreten sind:

- ☒ GD Grenada
- ☒ IN India

Erklärung bzgl. vorsorglicher Bestimmungen: Zusätzlich zu den oben genannten Bestimmungen nimmt der Anmelder nach Regel 4.9 Absatz b auch alle anderen nach dem PCT zulässigen Bestimmungen vor mit Ausnahme der im Zusatzfeld genannten Bestimmungen, die von dieser Erklärung ausgenommen sind. Der Anmelder erklärt, daß diese zusätzlichen Bestimmungen unter dem Vorbehalt einer Bestätigung stehen und jede zusätzliche Bestimmung, die vor Ablauf von 15 Monaten ab dem Prioritätsdatum nicht bestätigt wurde, nach Ablauf dieser Frist als vom Anmelder zurückgenommen gilt. *(Die Bestätigung einer Bestimmung erfolgt durch die Einreichung einer Mitteilung, in der diese Bestimmung angegeben wird, und die Zahlung der Bestimmungs- und der Bestätigungsgebühr. Die Bestätigung muß beim Anmeldeamt innerhalb der Frist von 15 Monaten eingehen.)*

A METHOD FOR A SECURE DETACH PROCEDURE IN A RADIO TELECOMMUNICATION NETWORK

FIELD OF THE INVENTION

The present invention relates to a method for performing a secure detach procedure in a radio telecommunication network, in particular in a so-called third generation network. Moreover, the present invention relates to a corresponding registration procedure for registering a subscriber to such a telecommunication network. Also, the present invention relates to corresponding devices of subscriber terminals and network controlling devices which are adapted to carry out these methods, and to a correspondingly adapted telecommunication network.

BACKGROUND OF THE INVENTION

In hitherto known telecommunication networks, a subscriber terminal as a first type radio transceiver device (hereinafter: mobile station MS), in order to be operated within a network, needs to be registered to the network NW, i.e. to a network controlling device like for example a mobile services switching center MSC (or an SGSN), which controls so called base station controllers BSC, which in turn control base stations BS as second type radio transceiver devices.

To this end, each subscriber has a subscriber identity module SIM to be inserted into the used mobile station MS as a respective terminal equipment. The SIM contains a pre-stored international mobile subscriber identity number IMSI, by which a user can be identified. However, in order to protect the user against being identified by an intruder

in the network, each user is assigned a temporary mobile subscriber identity TMSI. This identification which changes either from time to time or from area to area (when combined with a location area identifier LAI) allows an "anonymous" identification of the user when using his terminal.

For details of the roughly described registration procedure including ciphering of transmitted data for authentication at registration, which details are considered to be not necessarily to be described here, the reader is referred to the plurality of respective publicly available GSM specifications.

Likewise, an attached or registered subscriber or mobile station, respectively, will have to perform a detach from the network under specific conditions. For example, the mobile station will be detached from the network and its registration will be abandoned, in case the SIM module is detached from the terminal equipment or the like.

In such cases, the mobile station MS sends a detach message to the network NW, the so-called IMSI DETACH INDICATION message. Upon receipt of the IMSI DETACH INDICATION the network controlling device (MSC) sets an inactive indication for the mobile station MS, while no response is returned to the mobile station itself. (For details, also in this context it is referred to the respective GSM specifications). Namely, no authentication is conducted at detach, when the mobile station initiating the detach procedure leaves the network.

Thus, there exists a possibility that a malicious user may obstruct or even terminate a third party's call by sending detach messages with random identities of mobile stations

(i.e. random numbers of TMSI identifiers). Stated in other words, although it is not possible to interrupt the connection to a specific mobile station MS of a certain specified user by sending such a detach message, a lot of damage and irritation can be caused to a great number of users as well as to the operator of the network NW, when arbitrary calls and/or radio connections are blocked and/or terminated by the intention of a malicious third party.

A previously proposed approach to prevent this resides in performing an authentication procedure when a mobile station MS is to be detached from the network NW, i.e. upon receipt of a detach message at the network from the mobile station.

However, such a proposed authentication at detach is rather time consuming in many situations and has therefore only a limited applicability.

Moreover, performing an authentication procedure may not be feasible if the mobile station is performing power off, i.e. is switched off, or the available battery power is too low so that normal operation of the mobile station can not be assured any longer.

SUMMARY OF THE INVENTION

Hence, it is an object of the present invention to provide a simple and useful method for performing a detach from and/or a corresponding method for registration to a network, which prevent the above described problems.

According to the present invention, this object is achieved by a method for performing a detach of a terminal registered to a telecommunication network by

associating an identification for said terminal, deriving a signature for said identification, and allocating a pair consisting of said identification and said signature to said terminal, said method comprising the steps of: sending a detach request including said identification and said identification signature from said registered terminal to said network; receiving said detach request at the network side; comparing said received detach request with a record of registration data of said terminal kept at the network side; and detaching said terminal from said network, if said received detach request coincides with said record of registration data.

According to the present invention, this object is furthermore achieved by a method for registration of a terminal to a telecommunication network, said method comprising the steps of: associating an identification for said terminal, deriving a signature for said identification, and allocating a pair consisting of said identification and said signature to said terminal.

Favorable refinements of the present invention are as defined in the respective dependent claims.

Thus, the present invention provides the advantage that a simple and useful method is available for preventing a malicious user to interrupt third party's calls by sending detach messages with random identities of mobile stations.

In particular, the proposed method enables an immediate authentication of the mobile station requesting a detach procedure upon receipt of the detach request message or the detach request, respectively. This authentication procedure is not time consuming and also applicable in case of a mobile station being switched off (entering the power off

state) or having a battery level which is too low for normal operation of the mobile station. Thus, even in such situations, the detach procedure may be carried out correctly.

Moreover, due to the fact that the detach request is composed of the identifier as well as the identifier signature, the proposed immediate authentication process is highly secure, because in practice it is impossible to find such a matching pair by just taking two arbitrary numbers.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be more readily understood with reference to the accompanying drawings, in which:

Fig. 1 shows a flowchart of the registration procedure according to the present invention;

Fig. 2 shows a flowchart of the detach procedure according to the present invention; and

Fig. 3 shows a schematic representation of the data format used for the detach request or detach request message, respectively, according to the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

According to the present invention, when a mobile station MS as a first type radio transceiver station or, in general, a terminal is registered to a network NW like for example a so-called third generation radio telecommunication network, i.e. registered to the network controlling device MSC, it sends an attach/registration request (formed by one or more request messages), or

dependent on the specific situation, a location update request to the network NW. A request as such (to be valid for being evaluated) may be composed of more than one transmitted messages.

The network NW, which for the present description is assumed to be represented by the network controlling device as for example an MSC, in turn associates an identification to the mobile station MS. Associating such an identification may be achieved in that the network NW allocates an identification to the terminal MS

The identification may be represented by the temporary mobile subscriber identity TMSI. Alternatively, as the identification also the international mobile subscriber identity IMSI could be used. In general, any suitable identification may be used for identifying a respective mobile terminal MS, and the present invention is not restricted to the use of the TMSI or the IMSI as identifications.

Additionally, the network NW allocates a signature (e.g. TMSI signature TMSI_SIG) corresponding to the identification and derived therefor on the basis of, for example, a coding algorithm like an algorithm known as the "Pretty Good Privacy" (PGP) algorithm, to the terminal, i.e. the mobile station MS. However, the deriving of the signature for and/or of the identification is not limited to the network side. Namely, alternatively, also the terminal MS may derive a signature for the identification by way of calculation. In this connection, information as to which algorithm for calculating the signature is to be chosen is in such a case exchanged between the network NW and the terminal MS. After having thus derived the

signature, the deriving side (i.e. NW or MS) informs the other side of the derived signature.

Both data items, the identification TMSI as well as the identification signature TMSI_SIG are allocated to the mobile station MS in a secure mode, so that it is impossible for any other mobile station or any other third party to know the pair of these data items TMSI, TMSI_SIG. Of course, if in the above mentioned example case the terminal MS derives the signature, the derived signature is informed to the network NW in a secure mode, to be securely associated to the identification, so that it is impossible for any other mobile station or any other third party to know the pair of these data items TMSI, TMSI_SIG.

In particular, according to the present invention, the network NW or the network controlling device MSC, respectively, associates and/or allocates also a signature TMSI_SIG in combination with the identifier TMSI itself to the mobile station MS. Moreover, according to the present invention, the associated signature is used together with the identifier in a detach procedure, as described below.

Namely, in case the mobile station MS leaves the network NW and is to be detached therefrom due to, e.g., switching off the mobile station MS or a low battery charging state at the mobile station's side or a removal and/or taking off a SIM card (subscriber identity module) as examples for a respective predetermined detach condition for the mobile station, a detach procedure according to the present invention is performed. In particular, in this detach procedure, the mobile station MS when requesting and/or initiating detach, sends a detach request to the network NW. The detach request contains the identification TMSI and the identification signature TMSI_SIG as a pair of data

items. The network compares the received two data items which identify the requesting mobile station with the previously allocated one's. If the comparison yields that the received data items are identical to the previously allocated one's, the detach is performed correctly at the network side. Because no other mobile station MS except the one to which the identifier signature and corresponding identifier were previously allocated to, knows the pair of data items, it is impossible for other mobile stations to perform a malicious detach procedure.

The following description of the drawings will set out the operation of the present invention in greater detail.

Fig. 1 shows a flowchart of the registration procedure. In step S0 the registration procedure starts. In the subsequent step S1, it is checked at the mobile station MS side, whether a registration condition is present. Such a registration condition may for example be present when said mobile station newly attaches to a network NW and has initially to be registered (authenticated) at the network NW side, or when said mobile station has moved within the network NW and a location update of said mobile station MS becomes necessary. Alternatively, also a cell update in case of the terminal having moved to an extent that the previous cell has been left and a new cell was entered represents such a registration condition. Also, in third generation networks an URA (UTRAN Registration Area, UTRAN standing for "Universal Terrestrial Radio Access Network") update is possible, thus representing a registration condition in the sense of the present invention. Such an URA update may be necessary in case of third generation networks, in which a radio network controller RNC handles the location information in terms of registration areas.

Such updates become for example necessary when the mobile station has to be registered to another controlling device MSC within the network due to "excessive" moving within the network and/or in case of a request of the mobile station MS for a traffic channel assignment.

If no registration condition is present in step S1, the procedure returns to step S1 until a registration condition is present. Then, the process proceeds to step S2.

In step S2, the mobile station MS sends a registration request REG_REQ to the network NW, i.e. to the network controlling device, e.g. the MSC. The registration request REG_REQ is for example an attach request for initial registration of said mobile station MS as a first type radio transceiver device in said network, or a location update request for updating a previous registration of said mobile station MS in said network, or any other request which is transmitted when any of the above described further possible registration conditions is satisfied.

In step S3, this registration request REG_REQ is received by the network controlling device. In response to receiving said request, the network controlling device selects or determines an identification like for example TMSI for the requesting mobile station MS.

Moreover, in a subsequent step S4 of the described example, the network NW (network controlling device MSC) also derives an identification signature TMSI_SIG for said identification TMSI. (However, as mentioned above, the signature may also be derived by the mobile station MS itself upon receipt of a corresponding instruction from the network NW, and the signature will then have to be informed to the network NW (not represented in the figures).)

Both of these data items as parameters for identifying a specific mobile station MS, namely, the identification TMSI and the (separate) identification signature TMSI_SIG are allocated to the mobile station MS in a subsequent step S5. Of course, the network NW keeps a record of the thus assigned pair of data items.

The data items TMSI and TMSI_SIG are allocated in a secure mode, so that a third party may not obtain a knowledge of the assigned data items. Then, in step S6 of the described example, they are transmitted from the network NW side to the mobile station MS side in order to inform the mobile station of the allocated identification TMSI and the identification signature TMSI_SIG.

Thereafter, in step S7, the registration procedure is completed.

Fig. 2 illustrates a flowchart of the detach procedure when a mobile station MS as a terminal is to be detached from the network it has previously been registered to.

The detach procedure starts in a step S8. In a subsequent step S9, at a respective mobile station MS side, it is checked whether a predetermined condition, i.e. a detach condition, of the mobile station MS is present. Such a detach condition may for example be met in case of a power off state of said mobile station MS, or in case a low battery charging state of the battery of the mobile station is detected. Alternatively, a user actuated command may fulfill the detach condition, for example, if another user wishes to use the mobile station MS as a terminal equipment and an SIM module (subscriber identity module) of the new user has to be inserted. This applies also in case of removal of the SIM module.

If no such detach condition as a predetermined condition is detected, the procedure loops until a corresponding condition is detected. If a detach condition is detected at the mobile station side, the mobile station MS sends a detach request DET_REQ to the network NW, i.e. to the network controlling device like an MSC, step S10.

The detach request DET_REQ contains said pair of said identification TMSI and said identification signature TMSI_SIG previously allocated to said mobile station MS upon registration of the mobile station to the network NW.

In particular, the detach request DET_REQ, may for example, assume a data format as shown in Fig. 3 of the drawings. As roughly schematically illustrated therein, a burst transmitted from the mobile station MS to the network NW (controlling device) contains the detach request DET_REQ. The detach request contains the pair of the identification TMSI and the identification signature TMSI_SIG. Although the TMSI and TMSI_SIG are illustrated as being transmitted immediately one after the other in the burst, another burst format may be adopted in that there may be provided a guard period or dummy period (not shown) between the respective data items. Alternatively, each data item could be identified by a respective flag (not shown) indicating which data item is transmitted next, and transmitted prior to the respective data item. Moreover, in the latter case, the order of the specific transmitted data items would not be restricted to a specific one, but could be changed in an arbitrary manner, as long as the data items could be identified at the reception side. Furthermore, the detach request could be transmitted in a form such that for example, the identification and the identification signature could be transmitted in consecutive bursts as

respective request messages which in combination result in the request as such.

In step S11, the detach request DET_REQ is received at the network NW side. In a following step S12, the received detach request DET_REQ is compared, data item per data item, i.e. separately for the identification TMSI and the identification signature TMSI_SIG, with a record of registration data of said terminal kept at the network side. The record is the record of the previously assigned pair of data items TMSI, TMSI_SIG kept at the network NW side, as mentioned above in connection with step S5, upon registration of a respective mobile station MS to the network NW.

Namely, at the network controller side a set of such records (e.g. in form of a table) of all allocated pairs of data items TMSI, TMSI_SIG for all respective mobile stations currently registered to the network is kept, and in step S12 a check is made as to whether the received pair of TMSI, TMSI_SIG is contained as a record in said set of records (table).

If the pair of data items received with the detach request message DET_REQ is not contained in said record (NO in step S12), the procedure advances to step S13. In step S13, no detach operation is performed, and all registered mobile stations remain registered to the network. Also, an authentication procedure (registration) could then be started in this case in step S13. Therefore, a malicious user sending arbitrary identifications can not terminate any call or detach any other user, since he is not enabled to send a pair of matching data items of an identification TMSI and a corresponding identification signature TMSI_SIG.

If, however, the comparison in step S12 yields that the received detach request DET_REQ contains a pair of data items TMSI, TMSI_SIG which is contained in the table of records, i.e. has previously been allocated to a mobile station upon registration, (YES in step S12) then the flow proceeds to step S14.

In step S14, a detach operation is performed, since it has been verified that the detach request DET_REQ originated from an authentic mobile station which was previously registered to the network. Thus, an immediate authentication procedure can be carried out by comparing the pair of received data item TMSI, TMSI_SIG with a record of previously allocated (assigned) data items. This assures that a detach operation is only performed for a mobile station MS as a respective terminal, if the request for detach originates from the mobile station MS itself. Hence, no malicious user can initiate a detach of arbitrary mobile stations since he can not know the pair of the identification TMSI and the corresponding signature TMSI_SIG.

Moreover, the authentication at detach is immediately effected at the network side without involving a repeated handshaking procedure with the mobile station. Thus, the authentication procedure can also be successfully performed in case the mobile station has a too low battery charging level, has been switched off, or the like.

The procedure has been described herein above mainly with reference to the temporary mobile subscriber identity TMSI being used as an identification and for deriving the signature therefor, since the TMSI is already defined in existing radio telecommunication systems and, therefore, can be advantageously be used in connection with the

present invention. Nevertheless, the present invention can also be carried out in case a new identification and corresponding signature thereof are defined, while this, however, would require additional changes to existing agreed standards.

It should be understood that the above description and accompanying drawings are only intending to illustrate the present invention by way of example. Thus, the preferred embodiment of the invention may vary within the scope of the attached claims.

CLAIMS

1. A method for performing a detach of a terminal (**MS**) registered to a telecommunication network (**NW**) by associating an identification (**TMSI**) for said terminal (**MS**), deriving a signature (**TMSI_SIG**) for said identification (**TMSI**), and allocating a pair consisting of said identification (**TMSI**) and said signature (**TMSI_SIG**) to said terminal (**MS**),
said method comprising the steps of:
sending a detach request (**DET_REQ**) including said identification (**TMSI**) and said identification signature (**TMSI_SIG**) from said registered terminal (**MS**) to said network (**NW**);
receiving said detach request (**DET_REQ**) at the network (**NW**) side;
comparing said received detach request (**DET_REQ**) with a record of registration data of said terminal (**MS**) kept at the network side; and
detaching said terminal (**MS**) from said network (**NW**), if said received detach request (**DET_REQ**) coincides with said record of registration data.

2. A method according to claim 1, wherein
sending of said detach request message (**DET_REQ**) is initiated upon detection of a predetermined state of said terminal (**MS**).

3. A method according to claim 2, wherein
said predetermined state is a power off state.

4. A method according to claim 2, wherein
said predetermined state is a low battery state.

5. A method according to claim 2, wherein

said predetermined state resides in a removal of a SIM module from said terminal.

6. A method according to claim 1, wherein
said record of registration data contains said pair consisting of said identification (**TMSI**) and said identification signature (**TMSI_SIG**), and
said comparison is effected for each of said data items forming said pair.

7. A method according to claim 1, wherein
said identification (**TMSI**) is the temporary mobile subscriber identity.

8. A method according to claim 1, wherein
said identification is the international mobile subscriber identity IMSI.

9. A method for registration of a terminal (**MS**) to a telecommunication network (**NW**),
said method comprising the steps of:
associating an identification (**TMSI**) for said terminal (**MS**),
deriving a signature (**TMSI_SIG**) for said identification (**TMSI**), and
allocating a pair consisting of said identification (**TMSI**) and said signature (**TMSI_SIG**) to said terminal (**MS**).

10. A method according to claim 9, further comprising the step of
sending a registration request (**REG_REQ**) from said terminal (**MS**) to said network (**NW**); and wherein
said associating is effected in response to the receipt of said registration request.

11. A method according to claim 10, wherein said registration request (**REG_REQ**) is an attach request for initial registration of said terminal (**MS**) in said network (**NW**).

12. A method according to claim 10, wherein said registration request (**REG_REQ**) is a location update request for updating a previous registration of said terminal (**MS**) in said network (**NW**).

13. A method according to claim 10, wherein said registration request (**REG_REQ**) is a cell update request for updating a previous registration of said terminal (**MS**) in said network (**NW**).

14. A method according to claim 10, wherein said registration request (**REG_REQ**) is a URA update request for updating a previous registration of said terminal (**MS**) in said network (**NW**).

15. A method according to claim 9, wherein said associating of said identification (**TMSI**) is arbitrary.

16. A method according to claim 9, wherein said allocating is effected in a secure mode.

17. A method according to claim 9, wherein said identification (**TMSI**) is the temporary mobile subscriber identity.

18. A method according to claim 9, wherein said identification is the international mobile subscriber identity IMSI.

19. A terminal device adapted to the method according to any of claims 1 to 18.

20. A network controlling device adapted to the method according to any of claims 1 to 18.

21. A telecommunication system consisting of at least one terminal (MS) and at least one network controlling device controlling at least one radio transceiver device, adapted to carry out the method according to any of claims 1 to 18.

ABSTRACT

The present invention proposes a method for performing a detach of a terminal (**MS**) registered to a telecommunication network (**NW**) by associating an identification (**TMSI**) for said terminal (**MS**), deriving a signature (**TMSI_SIG**) for said identification (**TMSI**), and allocating a pair consisting of said identification (**TMSI**) and said signature (**TMSI_SIG**) to said terminal (**MS**), said method comprising the steps of: sending a detach request (**DET_REQ**) including said identification (**TMSI**) and said identification signature (**TMSI_SIG**) from said registered terminal (**MS**) to said network (**NW**); receiving said detach request (**DET_REQ**) at the network (**NW**) side; comparing said received detach request (**DET_REQ**) with a record of registration data of said terminal (**MS**) kept at the network side; and detaching said terminal (**MS**) from said network (**NW**), if said received detach request (**DET_REQ**) coincides with said record of registration data. Also, the present invention relates to a corresponding registration method and proposes a new format for a detach request message transmitted from a mobile station MS as a terminal to a network NW controlling device like an MSC, and also relates to correspondingly adapted devices.

- **FIG. 2** -

FIG. 1

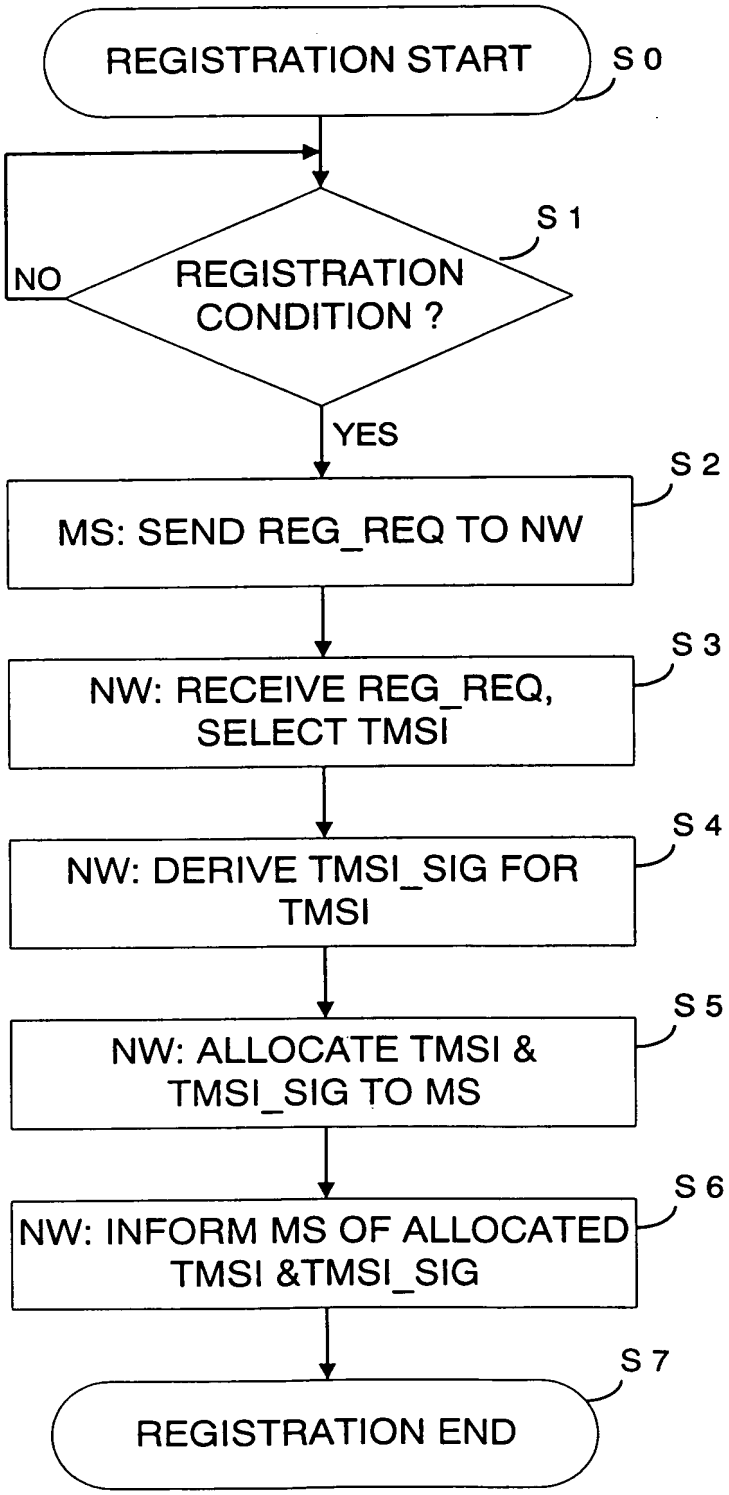
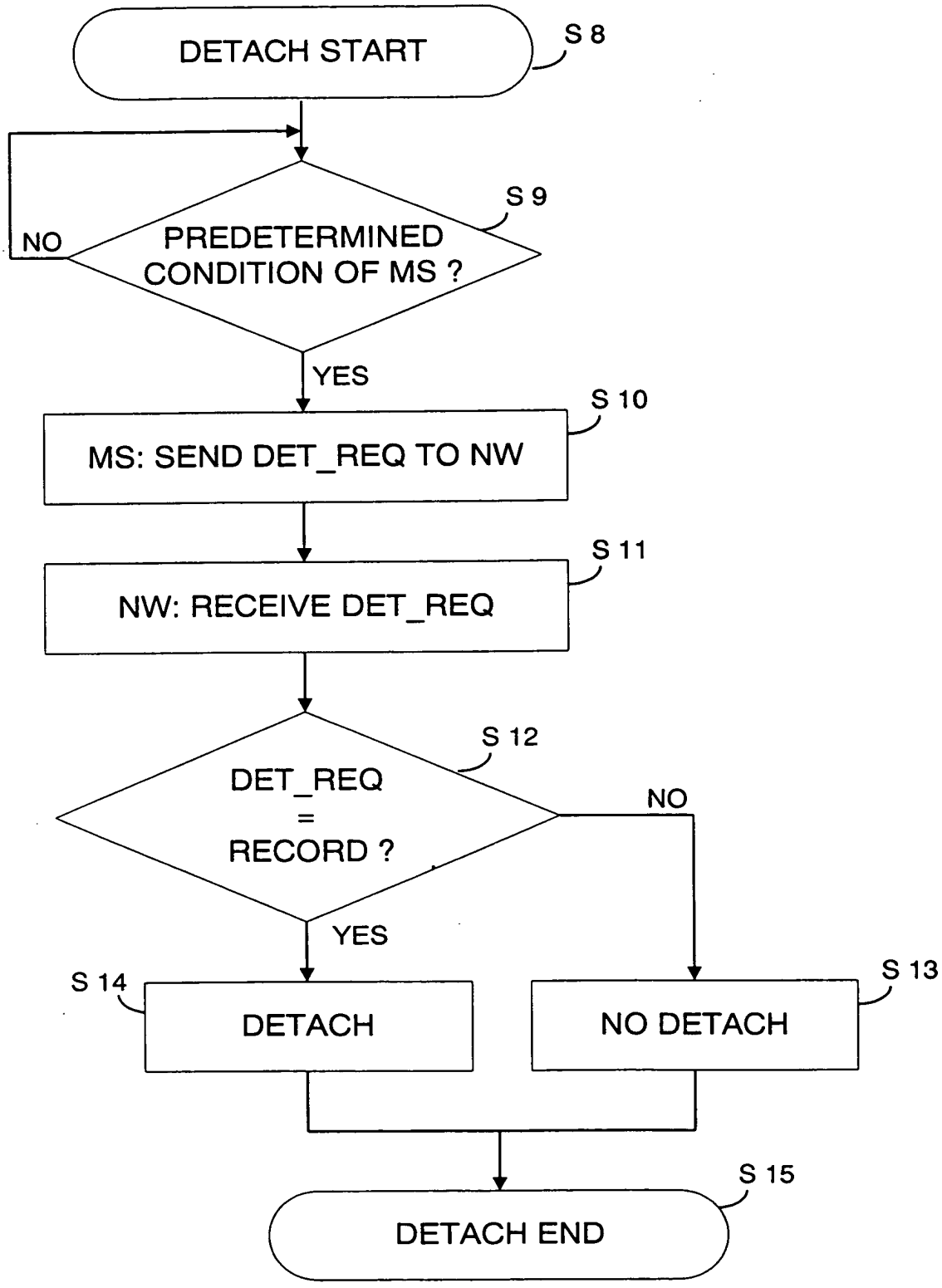

REGISTRATION START
S 0
S 1
NO
REGISTRATION CONDITION ?
YES
S 2
MS: SEND REG_REQ TO NW
S 3
NW: RECEIVE REG_REQ, SELECT TMSI
S 4
NW: DERIVE TMSI_SIG FOR TMSI
S 5
NW: ALLOCATE TMSI & TMSI_SIG TO MS
S 6
NW: INFORM MS OF ALLOCATED TMSI &TMSI_SIG
S 7
REGISTRATION END

FIG. 2


DETACH START
S 8
S 9
NO
PREDETERMINED CONDITION OF MS ?
YES
S 10
MS: SEND DET_REQ TO NW
S 11
NW: RECEIVE DET_REQ
S 12
DET_REQ = RECORD ?
NO
YES
S 14
DETACH
S 13
NO DETACH
S 15
DETACH END

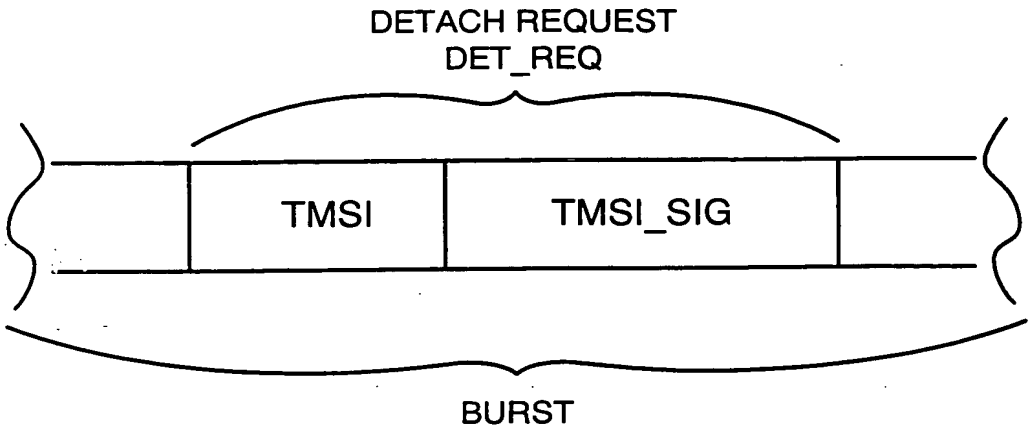



FIG. 3